Deloitte.

PSD2 - Payment Services Directive 2

What is new ?

1. Background

1.1 Context & timeline

The Revised Payment Services Directive (PSD2) follows in the footsteps of PSD, adopted in 2007, and is a fundamental stage in the implementation of the Single Euro Payments Area (SEPA). PSD2 opens the market to new payment actors and extends the scope of services. In doing so, it increases competition with the aim of making payments more innovative, efficient, swift and secure for consumers.

On 8 October 2015, the European Parliament adopted the European Commission's Directive, then validated by the European Council of Ministers in November, and finally published in the Official Journal of the EU on 23 December 2015. Following standard procedures for the implementation of Directives, the EU Member States now have two years to implement PSD2 into national legislation.

The European Banking Authority (EBA) has a mandate to provide Regulatory Technical Standards (RTS) for the implementation of specific provisions from PSD2. In this role, the EBA opened two separate consultation periods with relevant discussion papers: the first concentrating on strong customer authentication and secure communication, and the second focusing on cooperation and exchange of information for passporting. When drafting the RTS, the EBA will cooperate closely with the European Central Bank (ECB).

Figure 1. Timeline: from PSD1 to PSD2 implementation in Member States legislation

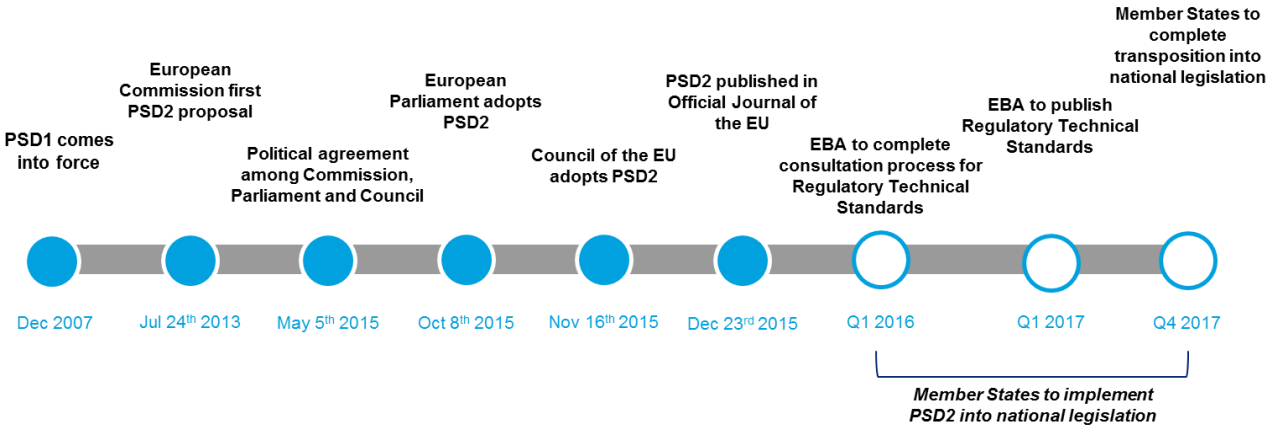
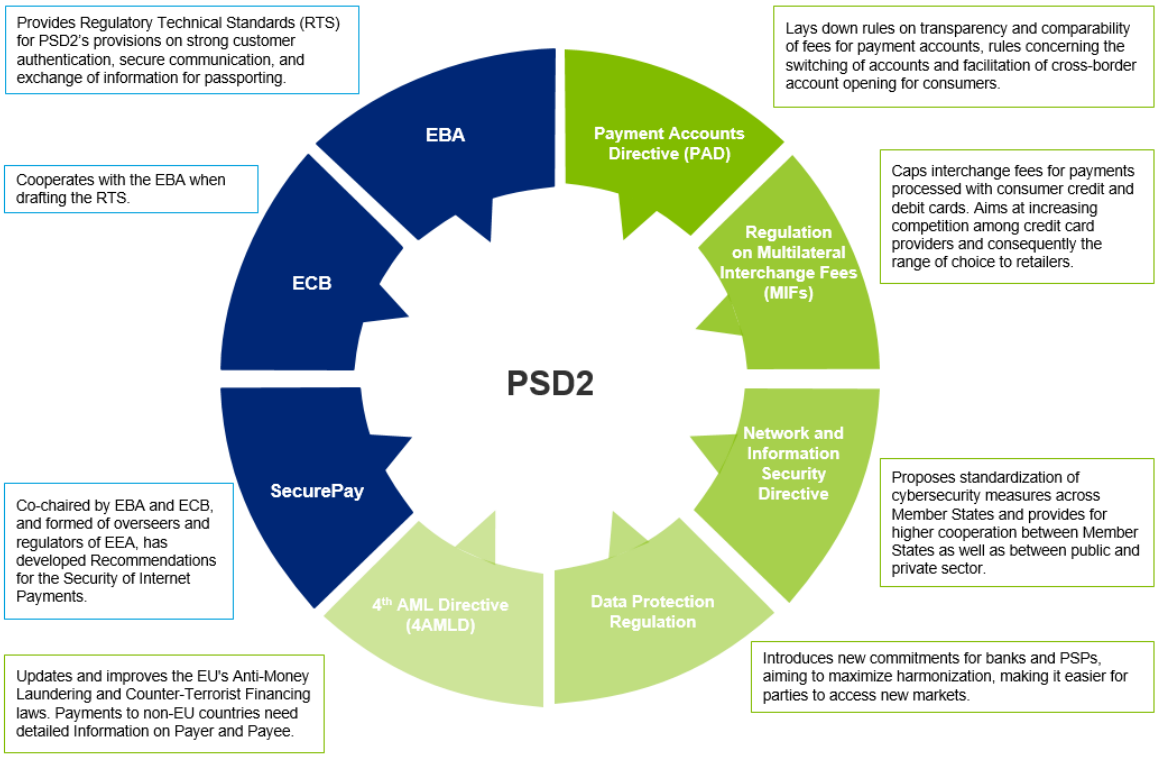


Figure 2. The stakeholders and regulatory framework around PSD2



1.2 Before PSD2

The original PSD, which regulated the payment industry before PSD2, allowed for payment services to be provided by banks, payment institutions (e.g. money remitters, retailers, phone companies) and e-money institutions. Together, these are categorized as Payment Service Providers (PSPs). PSD included provisions relating to fees, ensuring that customers were provided with all key information before and after payments. Customer protection solidly relied on harmonized refund rights in case of unauthorized debits, overcharge or incorrect processing. Furthermore, PSD was a fundamental step towards reducing the payment execution time to one day. The bank's agreement was required in order to access accounts and payments. Finally, PSD provisions only applied to payments when both payer and payee were located in the EU.

2. Key provisions

Since 2007, consumer payment and purchasing habits have changed significantly. Payment technologies are evolving and diversifying, and mobile devices are increasingly used to process payments. Within this context, and based on the regulatory framework laid down by PSD, PSD2 brings new provisions in the following areas:

→ Stakeholders

→ Scope of transactions

→ Liability

→ Access to accounts and security

2.1 New stakeholders

In a payments market where FinTech entities can provide payment initiation and consolidation services, PSD2 creates two new categories of PSPs: Account Information Service Providers (AISP) and Payment Initiation Service Providers (PISP). Together, they belong to the new set of PSPs referred to as Third Party Service Providers (TPSPs).

Currently, in order to have a holistic view of their financial situation, Payment Service Users (PSUs) with multiple accounts access each account separately through individual interfaces. AISPs enable PSUs to access account information from all accounts relevant to them. To allow this, PSD2 requires that – when permitted by the PSU – the bank grants access to the PSU's information to AISPs.

Today, the payer initiates the payment directly through its bank. With PSD2, PISPs will initiate payments through the bank's payment systems and infrastructure on behalf of the payers. This way PISPs act as a bridge between the payer and the payee. For the payers, this represents a significant advantage, as they no longer have to process their payment request through their banks. The payee benefits from these new services as well as they are immediately informed of the payment initiation and can instantly administer the dispatch of the purchased product. In its role, PISP will not receive or handle customer funds and will not provide account information, but will rather check, whether the payer has sufficient funds in his/her accounts to complete the transaction.

The regulation of these two new TPSPs entails new obligations for banks. When receiving a request from an AISP, banks should respond instantly, in a non-discriminatory way, and without thwarting the AISP's business. Payments processed through PISPs should be handled in the same way as those initiated through banks, without additional charges or lower priority. Neither AISPs nor PISPs will be forced to enter into a contract with banks in order to access information and initiate payments

respectively. These obligations, however, do not occur where a bank does not provide a transactional website for payment initiation, and only fully exist where banks provide a transactional website with both consultation and payment transaction tools. Where only a consultation platform is offered, banks have obligations towards AISPs only.

To enable TPSPs to connect directly to a PSU's bank, the EBA is developing new technical standards, specifically to define the connection requirements and API to be used. This requirement is referred to as "Access to Account" or XS2A, and will be published in 2016.

2.2 Expanded scope of transactions

As in PSD, all PSD2 provisions apply to payment services in the EU, and the provisions for transparency and information affect transactions in a Member State's currency where the PSP at both ends of the payment is located within the EU. Going beyond the former Directive, PSD2 extends the scope of the transparency and information requirements to transactions in any currency where only one of the PSP is within the EU ("one leg-out transactions"). These provisions apply to those parts of the payment chain that are carried out within the EU.

2.3 Liability

With new actors joining the payments value chain, PSD2 also ensures that they are protected against any liability with regards to the bank and PSU they are interacting with. To this end, both AISP and PISP are required to hold a professional indemnity insurance that covers all territories where they effect account information and payment initiation services.

PSD2 represents an essential step towards increased consumer protection in case of loss, theft, misappropriation, and incorrect execution. PSPs become fully responsible for proving that payments were (not) correctly executed, and are required to cover the ensuing reimbursement of the payment amount, as well as any related fees, charges or interests that the PSU may incur. Only where the PSU has acted fraudulently or out of gross negligence is it fully liable. Except for these cases, the highest fee a PSU can be liable for corresponds to €50, reduced from €150 in PSD.

2.4 Access to accounts and security

PSD2 provides that TPSPs access and use information on the PSU and its accounts only for the objective of processing the payment. This means that information cannot be stored, and that any personalized security credential should always be communicated among PSPs in a safe way.

A further change requested by PSD2 is the use of strong customer authentication. This entails the use of at least two out of three independent features in order to validate the identity of the PSU requesting the payment: knowledge (e.g. a password or security question), possession (e.g. a personal device, token, or digi-pass), and inherence (e.g. a fingerprint, an electrocardiogram, or retina data). The minimum requirement means that the violation of one of the two features does not compromise the trustworthiness of the other. Strong customer authentication is to be applied where the payer accesses its payment accounts online, initiates an electronic payment transaction, and carries out payments remotely. This new security requirement entails cooperation between the different PSPs, given that one PSP will rely on the other for the authentication procedures it may already provide to the PSU.

Finally, PSD2 requires that Member States implement a consistent incident reporting structure in case of major operational and security incidents. These reports are to be given to the competent authorities in the relevant Member State. Should the incident lead to a financial impact for the PSU, the latter

needs to be promptly notified. The EBA is responsible for preparing the guidelines according to which the PSP should classify incidents and authorities assess the reports.

3. Main impacts

The principal impacts of the upcoming PSD2-induced changes are six-fold:

1. New market players: Agile and flexible non-bank players will enter the payment services market, without the need to maintain heavy banking infrastructure or comply with complex legislations.
2. Evolution of the business model: Competition will intensify in parallel with a shift from profit-generating payment activities to new types of value-added services. Non-bank players, and merchants in particular, will be able to cherry-pick and focus on the most profitable services.
3. Enhanced services offerings: Innovative payment services will enhance the customer's experience.
4. New consumer-payments relationship: The transformation in payment services, including the possibility to use one single AISP to manage all of one's accounts, could lead to new consumer expectations regarding their other traditional banking offerings (e.g. decreased number of card transactions).
5. Organisational impact: Heavy IT changes are expected, from the opening of APIs to the new security requirements or improved server capacity at a minimum.
6. The above will affect the main stakeholders who could react both strategically and operationally:

   → **Banks:** strategically, they will have to select within a range of possible strategies, ranging from minimum compliance with PSD2 to proactive digital transformation to leverage the new opportunities introduced. They could for example consider setting up or collaborating with AISPs or PISPs. Furthermore, coupling PSD2 with the development of instant payments will incentivise banks to revisit their payment strategy and design partnerships with actors previously not considered within the payments ecosystem (e.g. telecommunication entities). Banks may also consider preparing an impact assessment on P&L to assess a potential threat to revenues, and should consider potential loss of revenues on payment cards businesses. Operationally, banks should consider the need for IT developments, including interoperability, strong customer authentication, XS2A, and online payments. Banks will also have to implement reporting and other regulatory requirements in particular for incident reporting.

   → **TPSPs:** strategically, they should account for the requirement to register as Payment Institutions, prepare an impact assessment on P&L, and ensure that professional indemnity insurance is subscribed to. Operationally, they may further develop technology infrastructure, including interfaces, XS2A, and security methods. They will also be subject to the same reporting requirements as banks.

   → **Merchants:** strategically, they should consider the opportunity to develop applications in order to offer a richer series of functions and services, including instant refunds, credit, receipt storage for expense management, and bank-hosted loyalty programs. Operationally, merchants will have to account for the technology infrastructures needed in order to ensure connections with PISPs to support the new payments workflow.

Our contacts

Pascal Eber
Partner | Operations Excellence
+352 451 452 649
peber@deloitte.lu

Eric Collard
Partner | Forensic & AML, Restructuring
+352 451 454 985
ecollard@deloitte.lu

Martin Flaunet
Partner | Banking Leader
+352 451 452 334
mflaunet@deloitte.lu

Patrick Laurent
Partner | Technology & Enterprise Application Leader
+352 451 454 170
palaurent@deloitte.lu

Basil Sommerfeld
Partner |
Operations Excellence & Human Capital
+352 451 452 646
bsommerfeld@deloitte.lu

Nam Vu,
Director |
Operations Excellence
+352 451 452 728
navu@deloitte.lu

Alexandre Havard
Senior Manager |
Operations Excellence
+352 451 453 148
ahavard@deloitte.lu

Giulia Bruni Roccia
Analyst |
Operations Excellence
+352 451 453 220
gbruniroccia@deloitte.lu

Deloitte Luxembourg
560, rue de Neudorf
L-2220 Luxembourg

Tel: +352 451 451
Fax: +352 451 452 401
www.deloitte.lu